

Backup and Restore Policy



The Thabachweu Local Municipality policies are statements of principles and practices dealing with the on-going management and administration of the Municipality's IT assets. These policies act as a guiding frame of reference for how the Municipality deals with everything from its day- to-day IT operational and support procedures to comply with security regulations and codes of practice. This "statement of purpose" will guide the actions to be taken to achieve that purpose.



Thabachweu Local Municipality

Table of Contents

1. Overview.....	2
2. Purpose.....	2
3. Scope	2
4. Definitions	3
5. Media Sets	3
6. Drive and Media	3
7. Backup schedules	4
7.1. Daily	4
7.2. Monthly	4
7.3. Data Archive	4
7.4. Remote / Online	4
8. Backup Media	4
8.1. Lifecycle policy.....	4
8.2. Decommissioning procedure.....	5
9. Roles and Responsibilities	5
10. Data Validation	5
11. Data Selection.....	5
12. Data Archive	6
13. Data Restoration.....	6
14. Offsite Storage.....	6
15. Corrective actions for non-policy compliance.....	6
16. Glossary and Abbreviations.....	7
Version Control.....	8
Author.....	8
Review	8
Approval	8



Thabachweu Local Municipality

1. Overview

This policy governs the backup process of the Thabachweu Local Municipality. The expected data to be backed up on servers include the Microsoft Active Directory Server, Windows Deployment Server, Sebata FMS data and user data stored on the server.

Backup of user and server data are created in case of a disaster affecting the servers or databases held on them. The backup solution is not intended for recovering individual files belonging to particular users from previous date in time. The backups are structured in the most efficient way for recovery complete systems and databases and therefore it makes the solution unsuitable and cumbersome for restoring individual items.

2. Purpose

This policy is designed to protect data of the Thabachweu Local Municipality and to ensure it can be recovered in the event of an equipment failure, intentional destruction of data, or disaster. To maintain the integrity and availability of information processing and communication services. Routine procedures should be established for carrying out the agreed back-up strategy, taking backup copies of data and rehearsing their timely restoration. The objective of the backups are to allow data essential to the Thabachweu Local Municipality to be restored or recovered as quickly as possible in the event of data loss or corruption on one or more of its computer systems

3. Scope

- To safeguard the information assets of the Thabachweu Local Municipality.
- To prevent the loss of data in the case of an accidental deletion or corruption of data, system failure, or disaster.
- To permit timely restoration of information and business processes, should such events occur.
- To manage and secure backup and restoration processes and the media employed in the process.
- Backup of the Municipality's entire software set shall be retained in such a manner that the computer operating systems and applications are fully recoverable. This will be achieved by using a combination of backup to disk, copy backups, full backups, differential backups, and transaction log backups.
- All work related data / information of the Municipality must be stored on the network drive to form a part of the backup process.
- Data stored on mobile computers and workstations will not be backed up via the server backup solution. Important data on mobile computers and workstations shall be backed up at the discretion of the end user using the Nero DVD backup utility installed on all the computers.
- Required backup documentation includes identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.



Thabachweu Local Municipality

- Documentation of the restoration process shall include procedures for the recovery from single-system or application failures, as well as for a total data center disaster scenario, if applicable.
- Backup and recovery documentation shall be reviewed and updated regularly to account for new technology, business changes, and migration of applications to alternative platforms.
- A full recovery process must be tested with the results documented on an annual basis.

4. Definitions

- Backup - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
- Archive - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
- Restore - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

5. Media Sets

The Municipality shall have 3 (three) media sets to fulfil the backup and restore requirement. The media sets that will be used are; daily, monthly and archived media sets each with their own lifecycle and retention process.

The data backup and restore software on the server shall be configured to comply with the following retention periods.

- Daily Media Set
 - 5 Days – Overwrite protection
 - 5 Days – Append protection
- Monthly Media Set
 - Never allow the tape to be overwritten with new data
 - Never allow append data to tape
 - Monthly media tapes will be kept for 5 years.
- Archived Media Set
 - Never allow the tape to be overwritten with new data
 - Never allow append data to tape
 - Archived media tapes will be kept for 10 years.

6. Drive and Media

The Municipality's tape drive shall be cleaned once a month and the cleaning cartridge shall be replaced every 3 (three) to 6 (six) months as the need arises.



Thabachweu Local Municipality

7. Backup schedules

Backups shall be done to tape for the daily, monthly and archived backup schedules. The data archiving backup schedule will be supported by an additional backup to an external storage device. This process forms a part of the Disaster Recovery Process and Business Continuity Plan.

7.1. Daily

- The daily backup process will start at 5pm and will stop before 7am the following day allowing a 14 hour backup to tape window.
- Verification of the data is not required on the daily backup schedule.

7.2. Monthly

- The monthly backup job will be created and configured separately from the daily backup job. The two backup job selections will be exactly the same however the data on the tape will need to be verified by the backup software.
- The monthly backup schedule will be done on tapes contained in the “daily media set”. After the backup schedule and data verification process successfully completes the tapes will be moved from the daily media set to the monthly media set.

7.3. Data Archive

- The data archive backup schedule will only be created once detailed information is obtained on the data that is scheduled to be archived. A detailed inventory report on the archived data must be filed in hard and soft copy for future reference.
- An external storage device will be used as a supplementary backup during the data archiving process. The backup to disk feature of the backup software will be used during this process to maintain the current share and security permissions.

7.4. Remote / Online

The Municipality will follow a parallel backup process to ensure data availability in case of a disaster. Remote / online backups of the Sebata - financial management system - data will be done via the internet to an approved service provider. This process shall be followed until such time when the data changes that occurred during that day exceeds the time to replicate that data to the services provider.

8. Backup Media

8.1. Lifecycle policy



Thabachweu Local Municipality

- Backup media / tapes may not be used more than 24 times in a 12 month period.
- Backup media / tapes will only have a 12 month usage lifecycle.
- Tape information such as age and backup cycle must be reviewed every 30 days to ensure compliancy.
- New backup media / tapes will be added to the “daily” media set and should the need arise will they be moved to the monthly or archive media sets.

8.2. Decommissioning procedure

- When backup media reaches either the 24 times used threshold or the 12 month age threshold the media must be decommissioned.
- The decommissioned media will be moved from the daily media set to the retired media set.
- The retired media must be destroyed / incinerated to ensure that it will not be possible to recover any information from the media.

9. Roles and Responsibilities

The Municipality’s Security Officer will at all times be accountable for the backup process. This process forms a crucial part in the Disaster Recovery Process and Business Continuity Plan.

The Security Officer may delegate the roles and responsibilities of this process to the Municipality’s IT support staff or to an external service provider.

10. Data Validation

The ability to restore data from the monthly and the archived tape sets must be tested and verified every 30 days. Only a partial restore shall be tested to an alternative location before the backup tapes are sent to the off-site location.

11. Data Selection

- SRVTHADC01
 - Windows Server Bare Metal Recovery
 - Active Directory system, server and service state
 - User shares and folders
 - Company shares and folders
- SRVTHADC02
 - Windows Server Bare Metal Recovery
 - Active Directory system, server and service state
 - All data related to the Windows Deployment Services



Thabachweu Local Municipality

- DHCP database
- SRVTHAFMS01
 - Sebata FMS Data
- SRVTHAFW01
 - Microsoft TMG rules and configurations

12. Data Archive

- The Municipality will follow the archiving process once a year during the month of December.
- The data scheduled for archiving will be backed up on 2 (two) tape sets and shall be clearly marked “archived media and the date the backup was done”.
- An additional backup will be done to an external storage device.
- The “data verification” option of the backup software must be used during this process.
- The tape media will be moved from their current media sets to the archived media for compliance purposes.
- A partial restore to an alternative location must be tested on the 2(two) tape sets. The content of the data must be validated as both accessible and usable.

13. Data Restoration

Users that require lost or corrupted files to be restored from backup must submit a request in writing to the Municipality’s Security Officer. The following information will be essential for the user data restore procedure:

- Document names, location or detailed information of the required data.
- Dates and times when last the data or documents was available, accessible with current information.
- Detailed dates and times when the data or documents were deleted, destroyed or corrupted.

14. Offsite Storage

- A minimum of 3 (three) full monthly backup versions of recoverable information must be stored in a secure, off-site location. An off-site location shall be in a secure space in a separate building, or with an off-site storage vendor approved by the Information Technology Security Office.
- The practice of taking backup media to the personal residence of ICT staff personnel is not permitted.
- Daily backup media shall be stored in a secure location; weekly backup media in the Municipality’s fireproof safe and monthly backup media in a secure location at the Municipality’s Disaster Management Centre or with an off-site backup storage service provider.

15. Corrective actions for non-policy compliance



Thabachweu Local Municipality

- Failure to comply with the guidelines stipulated in the Municipality's policies will result in the following corrective or disciplinary procedures.
- The decisive action that will be taken against the employee is dependent on the severity level and the level of the security risk.
- Warning from Management:
 - The employee receives a warning from their manager that they were in violation of policy.
- Written Warning in Personnel File
 - The employee is reprimanded, and official notice is put in their personnel file. This may have negative consequences during future performance reviews or promotion considerations.
- Revoking Privileges
 - Access to certain resources, such as internet or email, can be revoked for a limited period providing that this action does not have a negative impact on the employee's job functions.
- Training
 - Adequate training to create awareness and guidance on policy compliance.
- Disciplinary action will be determined in compliance to Schedule 8 of the Labour Relations Act 66 of 1995 or other related Public Service Regulations.

16. Glossary and Abbreviations

Please refer to the Thabachweu Glossary and abbreviations guide.



Thabachweu Local Municipality

Version Control

Version	State/Change	Author	Date
1.0	Original	Sbusiso Langa	
1.1	Changes	Sbusiso Langa	

Author

Name	Designation	Signature	Contact
Sbusiso Langa	Security Officer		+27 13 235 7367

Review

Name	Designation	signature	Date

Approval

Name	Designation	Signature	Date